Commonwealth of Massachusetts
Executive Office of Technology Services and Security (EOTSS)
Enterprise Security Office

Access Management Standard

Document Name: Access Management	Effective Date: October 15th, 2018
Document ID: IS.003	Last Revised Date: August 29, 2022

Table of contents

1. PURPOSE

1.1. **Access Management** — This ***standard*** defines the requirements for protecting the Commonwealth's ***information assets*** throughout their life cycle from the original request for access to the revocation of privileges. This standard addresses the following:

- User access management to verify authorized user access to ***information assets***
- User password management to control allocation of account passwords
- User responsibilities to prevent unauthorized access and compromise of ***information assets***
- Network access control to verify the security of network services and information assets
- System authentication control to verify authorized access to ***information assets***
- Provisioning of contractors' access to ***information assets*** through a formal management process

2. AUTHORITY

2.1. M.G.L. Ch. 7d provides that "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology."

3. SCOPE

3.1. This document applies to the use of information, information systems, electronic and computing devices, applications, and network resources used to conduct business on behalf of the Commonwealth. The document applies to all state agencies in the Executive Department including all executive offices, boards, commissions, agencies, departments, divisions, councils, and bureaus. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security, such as mass.gov, must agree to comply with this document as a condition of use. Executive Department agencies and offices are required to implement procedures that ensure their ***personnel*** comply with the requirements herein to safeguard information.

4. RESPONSIBILITY

4.1. The Enterprise Security Office Chief Information Security Officer (CISO) is responsible for the development and ongoing maintenance of this ***standard***.

4.2. The Enterprise Security Office is responsible for compliance with this ***standard*** and may enlist other departments in the maintaining and monitoring compliance with this ***standard***.

4.3. Any inquiries or comments regarding this ***standard*** shall be submitted to the Enterprise Security Office by sending an email to EOTSS-DL-Security Office.

4.4. Additional information regarding this document and its related ***policy*** and ***standards*** can be found at https://www.mass.gov/cybersecurity/policies.

5. COMPLIANCE

5.1. Compliance with this document is mandatory for the Executive Department including all executive offices, boards, commissions, agencies, departments, divisions, councils, and bureaus. Violations are subject to disciplinary action in accordance to applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

Exceptions to any part of this document must be requested via email to the Security Office (EOTSS-DL-Security Office). A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by the Commonwealth CISO or appointed desgnee.

6. STANDARD STATEMENTS

6.1. USER AND SYSTEM ACCESS MANAGEMENT

User or system access shall be managed throughout the account life cycle from the identification of a user to the granting, modification or revocation of a user's access privileges.

6.1.1. Allowed Access types: Access by Commonwealth accounts fall under the following categories:

6.1.1.1 Privileged access: Any account type that grants users elevated or increased application or information system capabilities that may affect computing systems; network communication; or the accounts, files, data or processes of Commonwealth systems, including the ability to read, update or distribute highly sensitive information or make changes to system configurations and security settings.

6.1.1.2 Interactive access: Any account type that allows one individual to log into an information system, through either a remote or direct connection, by entering appropriate credentials and supplying commands.

6.1.1.3 Non-interactive access: Any account type (i.e., non-human) used solely by a process, service or application to communicate with other systems.

6.1.1.4 Shared access: Any account type that is shared by two or more users or systems and may or may not provide the ability to associate a login or activity with a particular user or system (e.g., built-in account).

6.1.1.4.1. The creation and/or existence of non-built-in shared accounts must be managed as an exception using a formal risk management process. All exception-based shared account access should be time-boxed (where technically feasible), and the use of passwords should be controlled with an approval (e.g., Enterprise Security Office or agency CISO) driven checkout process. Passwords should be changed regularly and whenever a shared account member is removed from group access (see *Password Management in Access Management Standard*).

6.1.2. Allowed Account types: Allowed Commonwealth accounts fall under the following categories:

6.1.2.1 User account: A unique ID or login account owned by a single individual.

6.1.2.2 Administrator account: A privileged interactive account that is assigned to one and only one user. Passwords for these accounts must not be shared. Administrator accounts

provide individuals with a frequent need for elevated access to have the associated privileges and segment their regular access from the administrative access.

6.1.2.3 System account: A built-in account that enables administration, communications or processing services within infrastructure systems, platforms, applications and databases. Some system accounts are not intended for use by humans and are simply in place to start and stop various processes.

6.1.2.4 Service account: Interactive or non-interactive accounts that are not built in but are put in place by an organization to enable functionality such as communications or processing services within and between infrastructure systems, platforms, applications and databases. These types of accounts can also be used to grant specialized elevated rights to applications, systems or shared mailboxes.

6.1.2.5 Firecall (or breakglass) account: Interactive accounts with temporary privileged access rights that are intended for use on production systems by human users during operational, maintenance and troubleshooting activities.

6.1.2.5.1. Firecall accounts are managed via an automated or manual check-out process that requires an approved change control, service ticket, or other tangible business justification. Firecall accounts enable management of the environment and limit the need to directly access system accounts.

6.1.3. Prohibited Account Types: Prohibited Commonwealth accounts fall under the following categories:

6.1.3.1 Shared accounts: The creation and/or existence of non-built-in shared accounts is prohibited unless managed as an exception using a formal risk management process. All exception-based shared account access should be time-boxed (where technically feasible), and the use of passwords should be controlled with an approval (e.g., Enterprise Security Office or agency CISO) driven checkout process. Passwords should be changed regularly (see Password Management in Access Management Standard).

6.1.4. Where technically feasible (and available), certain types of privileged accounts shall be managed by a privileged access management (PAM) solution, maintained or approved by the Enterprise Security Office, or manual process, as follows:

Account type	Interactive	Shared	Control and Usage
Administrator	Yes	No	Administrator accounts are generally allocated to individuals; their use needs to be constrained by strong security policies. • PAM functionality: Not required although process to audit account access should be implemented • Example/use: account used to reset passwords
Service (a)	Yes	Yes	Service accounts have elevated rights but should generally not be shared unless required by business or technical constraints. • PAM functionality: Strong passwords, centrally manage passwords; password rotation • Example/use: Oracle DB account used to read data; accounts configured to enable particular functionality; accounts used to read log directories or manage group email lists
Service (b)	No	No	• PAM functionality: Enhanced monitoring • Example/use: Accounts used strictly for system-to-system calls to support regular operations
System (a)	Yes	Yes	The applicable controls required for system accounts are highly dependent on the operational nature of an application, the technical constraints, and underlying technology and/or vendor restrictions. • PAM functionality: Check-in, check-out; complex passwords; password rotation; and enhanced monitoring • Example/use: Sys DBA for Oracle; Root access for Unix (sudo)

System (b)	No	No	Some system accounts are non-interactive and do not allow login. • PAM functionality: Strong password (if applicable); enhanced monitoring • Example/use: accounts used strictly for system-to-system communication, potential use of certificate or key-pairs
Firecall	Yes	Yes	Firecall accounts are not allocated to individuals and are generally managed by a check-in/check-out process, and should also have strong passwords and increased monitoring. • PAM functionality: Check-in, check-out; password rotation; time-limit access • Example/use: emergency and temporary access to Production environments

6.1.5. Request access privileges: User requests for access privileges shall follow a formal process.

6.1.5.1 Commonwealth Executive Offices and Agencies must ensure that ***personnel*** sign and agree to the *Acceptable Use* Policy prior to obtaining any system access (see *Acceptable Use Policy)*.

6.1.5.2 User registration and revocation procedures shall be implemented for all ***information systems*** and services.

6.1.5.3 User access requests shall be recorded (paper or tool-based), include a business justification for access, and be approved by the requestor's supervisor and the appropriate ***Information Owner*** or authorized delegate.

6.1.6. Grant access privileges: Commonwealth Executive Offices and Agencies must ensure that Personnel with Security administration roles (hereafter, "***security administrators***") are responsible for the creation of accounts and the assignment of privileges after receiving the required access approvals.

6.1.6.1 Account managers: The Security Administrators perform the role of account managers for user access by creating, modifying, and revoking accounts, as well as serving as the point of contact for communications when user access needs change.

6.1.6.2 Access authorization: The ***Information Owner*** or ***Information Custodian*** shall verify that the type of access requested is required for the user's role and responsibilities.

6.1.6.3 Least privilege: Access shall be granted using the least privilege principle, i.e., only entitlements required to perform an individual's job responsibilities shall be granted.

6.1.6.4 Segregation of duties: The ***Information Owner*** shall confirm that conflicting access is separated to prevent fraud and/or misuse of the organization's assets.

6.1.6.5 Group and role membership: The Security Administrators shall determine the appropriate group and role membership of a user in the system based on the access request.

6.1.7. Modify access privileges: Upon the need for a change of user access, Commonwealth Executive Offices and Agencies must ensure that a user access request for change in access shall be recorded (paper or tool-based), include a business justification for change in access, and be approved by the requestor's supervisor and the appropriate Information Owner or authorized delegate.

6.1.7.1 Account managers shall be notified when system usage or need to know changes for an individual.

6.1.8. Revoke access privileges: Upon a transfer, termination or other significant change to a user's employment status or role, Commonwealth Executive Offices and Agencies must ensure that the user's previous supervisor shall be responsible for informing security administration personnel to take appropriate action.

6.1.8.1 Account managers shall be notified when accounts are no longer required, when users are terminated, when users are transferred, and when system usage or need to know changes for an individual.

6.1.8.2 Privileges that are no longer required by a user to fulfill his or her job role shall be removed.

6.1.8.3 If the termination date of ***personnel*** is known in advance, the respective access privileges — specifically those with access to ***confidential*** information — shall be configured to terminate automatically.

6.1.8.3.1. If not, access must be manually removed within 24 business hours.

6.1.8.4 ***Security administrators*** in consultation with the Enterprise Security Office (or agency's Information Security Team) may temporarily suspend or restrict a user's level of access to the network if his or her account is suspected of privilege abuse or violation of the *Acceptable Use* policy.

6.1.9. Monitor use of accounts: Account activity shall be monitored and reviewed in accordance with the Logging and Event Monitoring Standard.

6.1.10. Review of user access rights: Commonwealth Executive Offices and Agencies must ensure that ***security administrators*** shall maintain and review account access (either tool-based or manual) to verify that inactive and unauthorized accounts are appropriately de-provisioned.

6.1.10.1 Audit ***logs*** for account creation/ modification, deletion and access change shall be retained and reviewed in accordance with *the Logging and Event Monitoring Standard*.

6.1.10.2 A review of user's access must be conducted, at a minimum, semiannually, and all unauthorized accounts and access must be removed.

6.1.10.2.1. Login accounts inactive for 90 days must be disabled.

6.1.10.2.2. Disable accounts for personnel scheduled to go on an extended leave of absence of more than 90 days.

6.1.10.2.3. Remove or disable user accounts that no longer require access to ***information assets***.

6.1.10.2.4. Revoke access for any user no longer employed or under contract with a Commonwealth agency within 24 hours of notice.

6.1.10.2.5. More frequent reviews are encouraged commensurate to the risk level of the ***information asset*** or to meet regulatory requirements.

6.1.10.3 Privileged access reviews for Critical and High rated information systems shall be conducted by the ***Information Custodian*** or authorized delegate on a quarterly basis.

6.1.10.3.1. More frequent reviews are encouraged commensurate to the risk level of the ***information asset*** or to meet regulatory requirements.

6.1.11. Manage privilege access for system utilities: Access to system tools that have the capability to override system and application controls shall be restricted by Commonwealth Agencies and Offices to authorized personnel. All access to system utilities and tools shall be logged to facilitate the investigations of inappropriate use.

6.1.11.1 Privileged accounts (e.g., root or administrator level accounts) shall be used only for system administration where such access is required.

6.1.11.2 Administrative accounts shall not be used for non-administrative purposes (e.g., browsing the Internet).

6.1.11.3 Privileged user access shall be logged and monitored to prevent misuse of ***information assets***.

6.1.12. Emergency access management: Procedures shall be established (or implemented as needed) for obtaining necessary access to ***information assets*** during an emergency in accordance with *Business Continuity and Disaster Recovery Standard.*

6.1.12.1 Alignment with human resources termination and transfer process: On a periodic basis, Commonwealth Executive Offices and Agencies shall align account management processes with the personnel termination and transfer processes.

6.2. ACCOUNT MANAGEMENT

Commonwealth agencies and offices shall document and implement proper user identification and authentication processes, including:

6.2.1 Control and log the addition, deletion and modification of user IDs, credentials and other identifier objects.

6.2.2 Verify user identities prior to allowing password resets.

6.2.3 Require the use of a unique ID and ***two-factor authentication*** for system administration and other privileged access, including the management of network devices or ***information systems*** that contain ***confidential*** information, and for remote user access.

6.2.4 Disallow use of personal user accounts for administrative activities; as well, do not use administrative accounts for personal use.

6.2.5 Time-box and monitor accounts used by third parties for remote access.

6.2.6 Disconnect remote-access sessions after a specified period of inactivity (no longer than four (4) hours).

6.2.7 Restrict access to any database containing ***confidential*** information (including access by applications, administrators and all other users) by:

6.2.7.1 Limiting user access to, user queries of and user actions on databases to programmatic methods.

6.2.7.2 Limiting the ability to directly access databases containing ***confidential*** information to only database administrators and only for administrative purposes.

6.2.7.3 Limiting the use of application IDs for database applications to application processes (i.e., non-interactive).

6.2.8 Access attempts shall be limited by locking user IDs after no more than five (5) failed login attempts.

6.2.8.1 In the event a user account is locked out, the user must call the IT service desk to re-enable account access. A self-service password reset function managed and monitored by the Enterprise Security Office may be used.

6.2.8.2 "Reset account lockout counter after" policy shall be set to 30 minutes to mitigate against password timing and guessing attacks.

6.3.1 ***Information systems*** (e.g., operating systems, databases and applications) shall be configured with appropriate authentication controls designed to prevent unauthorized disclosure, modification or access to information.

6.3.2 Remote, wireless, and mobile access shall only be allowed for employees and contractors with a valid authorization, and shall be provisioned by Security Administrators in alignment with approved configurations.

6.3.3 No system or database containing non-public information shall be directly accessible from an untrusted network or ***information system***.

6.3.4 Logon processes shall be customized wherever possible to display only the information required for the user to authenticate. Minimal information about the ***information system*** shall be disclosed to avoid providing an unauthorized user with contextual information.

6.3.5 Workstations left unattended for extended periods of time must be locked or logged off.

6.3.6 The time-out delay shall reflect the security risks of the system, the classification of the information being handled and the risks related to the users of the system.

6.3.7 An automatic screen saver lock shall be configured to become active no more than five (5) minutes after inactivity for workstations used by ***personnel*** with access to any Commonwealth network and information system.

6.3.6.1 Put devices into a sleep or locked mode any time they are not in active use.

6.3.7 Network devices and systems shall be configured with appropriate access controls to prevent unauthorized modification or access to ***information assets*** and internal and external networked devices (See *Network Security Management in the Communications and Network Security* Standard).

6.3.8 Other than use of publicly available websites and systems, no user actions can be performed within systems without identification and authentication of the user.

6.4 Password Management

Commonwealth Executive Offices and Agencies must ensure that systems and processes to manage the enforcement of password controls for access to the network, operating systems, databases or applications shall be interactive and require strong passwords.

6.4.1 Passwords shall be configured securely using complexity and expiration requirements, as follows:

6.4.1.1 User passwords must be a minimum of twelve (12) characters and contain three (3) of the following four (4) characteristics:

6.4.1.1.1. Special characters (e.g., ‘, %, $, #)

6.4.1.1.2. Numerical characters (e.g., 1, 2, 3)

6.4.1.1.3. Alphabetic characters (e.g., a, b, c)

6.4.1.1.4. Combination of uppercase and lowercase letters

6.4.1.2 Passwords shall not use repeating, ascending, or descending character sequences (e.g., 12345, or abcde).

6.4.1.3 Passwords shall not use common words found in a dictionary, contain any part of a user's name, or the organization's name. The use of a "passphrase" is recommended, such as:
Tcopire2d! – A passphrase that is easy to remember as The cracking of passwords is ridiculously easy 2 do!
More info on passphrases can be found in the glossary.

6.4.1.4 Passwords shall not be the same as any of the last nine previously used passwords.

6.4.1.5 Privileged accounts (e.g., administrator) passwords shall consist of a minimum of fifteen (15) characters and contain the four (4) characteristics mentioned above.

6.4.1.5.1. If the system is limited to less than fifteen (15) alphanumeric characters, then the administrator's password length must be set to the maximum number of characters allowed by the operating system or application.

6.4.1.5.2. If it is less than eight (8) alphanumeric characters, an exception shall be submitted to the Commonwealth CISO for consideration.

6.4.1.6 For instances of ***two-factor authentication,*** user defined Personal Identification Numbers (PINs) must be a minimum length of at least eight (8) characters. This PIN will be used in conjunction with a six-digit randomly generated token PIN.

6.4.1.6.1. Authentication mechanisms (e.g., hard or soft tokens) must be assigned to an individual account and not shared among multiple accounts.

6.4.1.6.2. Physical and/or logical controls must be in place to confirm that only the intended account can use that mechanism to gain access.

6.4.1.7 Password must expire or change, as follows:

6.4.1.7.1. Require change of initial (or temporary) password upon first-time login/use. Initial passwords shall be unique for each user and received in a secure manner.

6.4.1.7.2. Passwords/PINs must be changed immediately if a compromise is suspected.

6.4.1.7.3. User accounts must be changed at least once every 90 days and administrator accounts must be changed at least once every 45 days.

6.4.1.7.4. Enforce a minimum password age of at least one (1) day.

6.4.1.7.5. Service account passwords must be changed at least annually.

6.4.2. PINs used with approved ***two-factor authentication*** solutions do not have to be regularly changed. Passwords for IDs used for non-interactive system access (e.g., IBM Mainframe batch IDs, Microsoft Windows service accounts or password disabled Unix IDs) may be exempt from the 90-day password change requirement. The system-specific technical standards shall be referenced for additional and/or qualifying controls.

6.4.3. Commonwealth Executive Offices and Agencies must ensure that one-time use and temporary passwords must adhere to the following:

6.4.3.1 Passwords must not be sent via fax.

6.4.3.2 Passwords must not be sent via email unless the email is encrypted.

6.4.3.3 Passwords must not be given via telephone unless the password administrator has positively identified the caller's identity.

6.4.3.4 Initial or temporary passwords must be forced to be changed immediately upon their first use.

6.4.3.5 Initial passwords must be in compliance with password composition and password selection requirements noted in this standard.

6.4.4. Commonwealth Executive Offices and Agencies must ensure that ***security administrators*** must positively identify the identity of a user prior to a password reset.

6.4.4.1 Only the individual to whom the user ID is assigned can request a password reset.

6.4.4.2 Password resets shall not be performed prior to verification of the requestor's identity.

6.4.4.3 If a self-service portal is not available, a "reset" password shall function as a one-time password required to be changed upon first use or login.

6.4.5. A user ID and password shall be authenticated in its entirety. If authentication fails, the system error message shall not indicate which component of the user's input (user ID or password) is incorrect (e.g., "incorrect login," or "incorrect password").

6.4.6. Passwords usage and storage must be secure.

6.4.6.1 Default passwords for software or hardware shall be disabled or changed.

6.4.6.2 Where technically feasible, password filtering and password masking shall be implemented.

6.4.6.3 Password credentials shall be encrypted and shall never be transmitted in clear text.

6.4.6.4 Password files shall be stored in an encrypted form separate from the object or application data they protect.

6.4.6.5 Users must not share or reveal passwords to anyone.

7. CONTROL MAPPINGS

Section	NIST SP800-53 R4 (1)	CIS 18 v8	NIST CSF
7.1 User and System Access Management	AC-1	-	ID.GV-1
	AC-2	CSC 5	PR.AC-1
	AC-3	CSC 5	PR.AC-4
	AC-5	CSC 5	PR.AC-4
	AC-6	CSC 5	PR.AC-4
	CM-5	CSC 4	PR.IP-1
	IA-2	CSC 16	PR.AC-1
	IA-8	CSC 16	PR.AC-1
	IA-9	CSC 16	PR.AC-1
	AC-21	-	PR.IP-8
	IA-1	-	ID.GV-1
		CSC 5	PR.PT-3
7.2 Account Management	AC-7	-	-
	AC-8	-	-
	AC-9	-	-
	AC-11	-	-
	AC-12	-	-
	AC-14	-	-
	AC-17	CSC 6	PR.AC-3
	AC-18	CSC 4	-
	AC-19	CSC 4	DE.CM-5
	IA-2	CSC 5	PR.AC-1
	IA-4	CSC 5	PR.AC-1
	IA-5	CSC 5	PR.AC-1
	IA-6	CSC 4	PR.AC-1
	IA-10	CSC 4	PR.AC-1
	IA-11	-	-
	PE-2	-	PR.AC-2
	PE-3	-	PR.AC-2
	SC-10	-	-
	AC-23	-	-
	AC-25	-	-
7.3 Password Management	IA-2	CSC 5	PR.AC-1
	IA-5	CSC 5	PR.AC-1

8. RELATED DOCUMENTS

Document	Effective date

9. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.9	Jim Cusson	10/01/2017	Corrections and formatting.
0.95	John Merto	12/22/2017	Edits;fixed numbering
0.96	Sean Vinck	5/7/2018	Corrections and Formatting
0.97	Andrew Rudder	5/31/2018	Corrections and Formatting
0.98	Anthony O'Neill	05/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	06/01/2018	Final Pre-publication Review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto
1.1	Megan Perkins	7/15/2020	Annual Review; Minor corrections and formatting
1.2	Sean M. Hughes	11/04/2021	Annual Review
1.3	Sean M. Hughes	08/29/2022	NIST 800-53R5 mapping and annual review

The owner of this document is the Commonwealth CISO (or designee). It is the responsibility of the document owner to maintain, update and communicate the content of this document. Questions or suggestions for improvement shall be submitted to the document owner.

9.1 Annual Review

This *Access Management* standard shall be reviewed and updated by the document owner on an annual basis or when significant policy or procedure changes necessitate an amendment.